UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/577,857	03/30/2007	Rached Ksontini	90500D-000083/US	4881

30593 7590 02/23/2010

HARNESS, DICKEY & PIERCE, P.L.C.
P.O. BOX 8910
RESTON, VA 20195

EXAMINER	
VAUGHAN, MICHAEL R	
ART UNIT	PAPER NUMBER
2431	
MAIL DATE	DELIVERY MODE
02/23/2010	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/577,857	KSONTINI ET AL.	
	Examiner	Art Unit	
	MICHAEL R. VAUGHAN	2431	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *04 December 2009*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-20* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-20* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

The instant application having Application No. 10/577857 is presented for examination by the examiner. Claims 1-20 are pending. Claim 20 is newly added.

Response to Amendment

Double Patenting

Examiner acknowledges Applicant's response to the double patenting rejection. Examiner will maintain that rejection as cited in the Office Action filed 9/8/08 until either the claims are amended enough to differentiate the conflicting claims or a terminal disclaimer is filed.

Claims 1-6, 8-11, 13, and 16-18 are provisionally rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claims 21-26, 29, 32, 33, and 36-40 of copending Application No. 10/577158. The detailed analysis of this rejection can be found in the Office action dated 09/08/2008.

Response to Arguments

Applicant's arguments filed 12/04/09 have been fully considered but they are not persuasive. The following interpretation of the prior art is solely based on the current set of claims and arguments submitted by the Applicant. It is not the only possible

interpretation of the prior art and may be altered when/if the claims and/or arguments change.

Applicant has alleged that the claimed invention is different from the cited art, Minemura, in that the instructions intended for the security module are generated by the server. Examiner respectfully disagrees because Minemura teaches that the instructions intended for the security module are generated by the server (0144). Starting from (0125), Minemura teaches that application-usable resource information governs what local resources the application has access to. In (0137), it is taught that this application-usable resource information is downloading with the application. Figure 15, shows the cryptogram including the application, the digest, and the application-usable resource information. Also see paragraph 0138. Furthermore, Minemura teaches a use license is part of the application-usable resource information (0141). And lastly Minemura teaches that the use license can be downloaded from the server (0144). Thus the application-usable resource information is taught by Minemura to be generated by the server. Therefore, the rejection under 35 USC 103 must be maintained.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said

subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-11 and 13-20 are rejected under 35 U.S.C. 103(a) as being unpatentable over USP Application Publication 2003/0114144 to Minemura in view of USP 6,832,230 to Zilliacus et al., hereinafter Zilliacus.

As per claim 1, Minemura teaches an authentication method of at least one application working in a equipment [terminal] connected by a network to a control server [server/service company], said equipment being locally connected to a security module [authentication module], said application being at least one of loaded loadable and executable via an application execution environment of the equipment and being adapted to use resources stored in the security module, the method comprising (see abstract):

analyzing and verifying by the control server of said data (0192),

generating by the control server a cryptogram comprising a digest of the application (0084-0085 and Fig. 6), and instructions intended for said module (0125),

transmitting the application and the cryptogram, via the network and the equipment, to the security module (0085), and

verifying, by the security module, the application by comparing the digest extracted from the cryptogram received with a digest determined by the security module (0085),

wherein, during at least one of initialization and activation of the application, the security module executes the instructions extracted from the cryptogram and, according to a result of the verification of the application, performs at least one of releasing and blocking access of certain resources of said security module to the application (0085). Minemura is silent in explicitly disclosing that the reception by the control server, via the network, of data comprising at least the identifier of the equipment and the identifier of the security module and that the cryptogram from the server includes these entities as well. Minemura does disclose teaching identifying data to the server from the terminal but not these specific entities. Zilliacus discloses sending these specific entities, the SIM and IMEI information to a control to authorize and authenticate a user terminal for downloading of content (col. 7, lines 15-25). Minemura teaches that the server send authorization information to terminal whereby it compares said information to information stored in the TRM in order to detect tampering (0088). The IMEI and SIM information are stored in a 'TRM'. Therefore it would have been obvious to send the SIM and IMEI to security module as well. Minemura teaching focuses on making sure that downloaded applications have not been tampered. Zilliacus emphasizes the mobile terminal's authentication to the server. One or ordinary skill in the art could have combined the two teachings to increase security whereby mutual authentication used to protect both the server and terminal.

As per claim 2, Minemura teaches the equipment is a mobile equipment of mobile telephony (0013).

As per claim 3, Minemura does not explicitly the network is a mobile network of at least one GSM or GPRS or UMTS (0013). Zilliacus teaches the network is a mobile network of at least one GSM or GPRS or UMTS (col. 5, lines 20-35). Minemura's invention is in the mobile telephony art. GSM is one specific type of mobile communication. Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to implement Minemura's system on a GSM network.

As per claim 4, Minemura teaches the security module is a subscriber module inserted into the mobile equipment of mobile telephony of the SIM card type (0013).

As per claim 5, Minemura teaches the identification of at least one of the set mobile equipment and subscriber module is carried out from the identifier of the mobile equipment and from the identifier of the subscriber module suited to a subscriber to the network (0193).

As per claim 6, Minemura teaches the instructions included in the cryptogram received by the security module condition the use of the applications according to criteria established previously by at least one of the operator, the application supplier, and the user of the equipment (0125, 0141).

As per claim 7, Minemura teaches the criteria define limits of use of an application according to the risks associated with at least one of the software of said application and with the hardware of the equipment that the operator desires to take into account (0125, 0141 and solves the problem of 0008).

As per claim 8, Minemura teaches the verification of the application with the cryptogram is carried out at the time of at least one of the first initialization and the first use of said application (0210).

As per claim 9, Minemura teaches the verification of the application with the cryptogram is periodically carried out at a given rate [expiry rate] according to instructions originating from the control server (0143-0144).

As per claim 10, Minemura teaches the verification of the application with the cryptogram is carried out at the time of each initialization of said application on the equipment (0144).

As per claim 11, Minemura teaches the cryptogram is generated with the aid of an asymmetrical or symmetrical encryption key from a data set (0199) containing, among other data, the identifier of the equipment, the identifier of the security module, an identifier of the application (0141), the digest of the application calculated with an unidirectional hash function and identifiers of the resources of the security module and instructions for locking/releasing of resources of the security module (0191).

As per claim 13, Minemura teaches the security module transmits to the control server, via the equipment and the network, a confirmation message when said security module has accepted or refused a cryptogram of an application (0087, provision of service).

As per claim 14, Minemura teaches the cryptogram is transmitted to the security module at the same time as the application is loaded into the equipment via the execution environment of the applications (0210).

As per claim 15, Minemura teaches the application, once loaded into the equipment from the control server via the network, requests a cryptogram from the server at the time of its initialization and transmits said cryptogram to the security module (0089), the confirmation message of acceptance or refusal of the cryptogram being transmitted by the security module to the server via the application (0210).

As per claim 16, Minemura teaches the equipment is a Pay-TV decoder or a computer to which the security module is connected (0078).

As per claim 17, Minemura teaches a security module [authentication module] comprising resources intended to be accessed locally by at least one application installed in an equipment [terminal] connected to a network (see abstract),

said equipment including means for reading and transmitting data (0085),

said module further including means for reception, storage, and analysis of a cryptogram and of the at least one application received with the cryptogram (Figure 6)

wherein the cryptogram includes, a digest of said application (0193) and instructions (0125),

means for verification of said at least one application (0192), and

means for extraction and execution of the instructions contained in the cryptogram, the means for extraction and execution performing at least one of blocking certain resources of the security module to the at least one application according to a result of the verification of the at least one application (0085-0089).

Minemura is silent in explicitly disclosing that the data includes at least the

identifier of the equipment and the identifier of the security module and that the cryptogram from the server includes these entities as well. Minemura does disclose teaching identifying data to the server from the terminal but not these specific entities. Zilliacus discloses sending these specific entities, the SIM and IMEI information to a control to authorize and authenticate a user terminal for downloading of content (col. 7, lines 15-25). Minemura teaching focuses on making sure that downloaded applications have not been tampered. Zilliacus emphasizes the mobile terminal's authentication to the server. One or ordinary skill in the art could have combined the two teachings to increase security whereby mutual authentication used to protect both the server and terminal.

As per claim 18, Minemura teaches the security module [IC] is at least one being of the "subscriber module" and "SIM card" type intended to be connected to a mobile equipment (0013).

As per claim 19, Minemura teaches the security module is a subscriber identification module [IC] inserted into the mobile equipment of mobile telephony (0013).

As per claim 20, Minemura teaches the cryptogram generated by the control server further includes at least one of an identifier of the application [signature; 0141]. Minemura is silent in explicitly teaching the cryptogram generated by the control server further an identifier of SIM resources. Zilliacus discloses sending these specific entities, the SIM and IMEI information to a control to authorize and authenticate a user terminal

for downloading of content (col. 7, lines 15-25). Examiner supplies the same rationale for combining Minemura and Zilliacus as recited in the rejection of claim 1.

Claim 12 is rejected under 35 U.S.C. 103(a) as being unpatentable over Minemura and Zilliacus as applied to claim 11 and in further view of USP Application Publication 2002/0012433 and to Haverinen et al, hereinafter Haverinen.

As per claim 12, Minemura is silent in disclosing a predictable variable in the cryptogram. Minemura does teach using a random number to prevent replay attacks (0192). Haverinen teaches that timestamps can be used as a substitute to random number in authentication to prevent replay attacks. Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to use the timestamps in the cryptograms as a means to prevent malicious replay attacks by a third party. Timestamps are known to be an adequate method of performing the same function of a random number in the art of computer security.

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to MICHAEL R. VAUGHAN whose telephone number is (571)270-7316. The examiner can normally be reached on Monday - Thursday, 7:30am - 5:00pm, EST. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, William Korzuch can be reached on 571-272-7589. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/M. R. V./

Examiner, Art Unit 2431

/William R. Korzuch/

Supervisory Patent Examiner, Art Unit 2431